[2345/97]

ENCRYPTION METHOD AND DEVICE

FIELD OF THE INVENTION

The invention relates to a method for encryption and to a device for implementing the method according to the precharacterizing portion of Claim 1 and Claim 5, respectively.

BACKGROUND INFORMATION

Modern encryption methods are being increasingly employed in information processing and telecommunication engineering. However, the use of encryption methods and corresponding devices is persistently impeded by the below-described problems and factors, although mass proliferation, particularly in the multimedia sector and in the field of information processing, calls for a very high standard of security:

- The encryption of broad-band signals requires the installation of costly crypto-hardware in personal computers and terminals. The currently available low-cost crypto-chipcards operate only at a low throughput rate of significantly less than 100 kbit/s.

- Encryption methods are often protected by property rights and not internationally standardized, so that no low-cost mass products with integrated crypto-hardware are available.

- For reasons of cost, crypto-hardware for broad-band encryption frequently employs just one encryption method. Consequently, the personal computers and other terminals equipped with one of these methods are not able to support any number of encryption

methods. This results in a great restriction in the compatibility of the indicated devices.

- Crypto-hardware is subject to strict international trade restrictions, with the result that the export, for example, of encryption terminals is very greatly restricted, which is why the use of such devices is very greatly limited and the prices for these devices are very high.

The book by Alfred Beutelspacher: *"Kryptologie"*, Vieweg Verlag, 1993, describes and presents encryption methods such as the Vernam cipher. In addition, encryption methods such as the RSA method are described in ITU/CCITT Recommendations X.509 and in CACM Communications of the ACM, Vol. 21, No. 2. pp. 120-126, 1978.

SUMMARY OF THE INVENTION

~~The~~ An object of the present invention is to create a method and a device for encryption, ~~the~~ an aim being to realize simplified implementation while avoiding expensive and incompatible broad-band encryption hardware, so that in the future, low-cost mass products can be equipped with integrated crypto-hardware, this considerably improving the standard of security of such products.

The design approach of the present invention for the method is characterized in the characterizing part of Claim 1.

Further embodiments or refinements of the method according to the invention are disclosed in the characterizing parts of Claims 2 through 4.

The design approach for implementing the encryption

methods and the device, respectively, is characterized in the characterizing part of Claim 5. Further refinements of the device are characterized in the characterizing parts of claims 6 and 7.

An present advantage of the design approach according to the invention is that the encryptors may operate with the same Vernam cipher (e.g. EXOR). They can be used without problem even when the external crypto- or PCMCIA modules (e.g. a multifunctional PC interface adapter) employ different symmetrical and asymmetrical ciphers. The Vernam cipher can also be implemented in software for high throughput rates, so that all encryptors are able to get along without the need for expensive crypto-hardware and can be used cost-effectively in mass products because their manufacture is technologically simple. The external crypto-modules likewise remain competitively priced because the Vernam key, produced in reserve, can also be generated by a low-performance or low-speed chipcard, for example for reserve in the Vernam-key storage, without slowing down the actual broad-band encryption process operating independently thereof.

Because of the method described herein, the encryptors are freed from the problems of expensive, high-performance and mutually incompatible crypto-hardware. By contrast, the Vernam cipher can be implemented very simply and cost-effectively in software, and consequently by storage. Complex crypto-functions are located outside of the encryptor. They are interchangeable by module and can be implemented in the proposed, competitively priced and low-speed external crypto-modules, such as the chipcard or the PCMCIA card, for example. The methods used are negotiated or "signaled" during coordination between sender and receiver, for example on

the transmission path. The encryptor itself ~~is~~ may be composed merely of software, such as, for example, PC software, or any other terminal/information system with an integrated Vernam cipher which does not need to be supported by expensive crypto-hardware for the actual encryption process.

Following, the invention is described in greater detail with reference to exemplary embodiments shown in principle in the drawing, in which:

Fig. 1 shows a known Vernam cipher represented in simplified form;

Fig. 2 shows a modern, known symmetrical cipher;

Fig. 3 shows a configuration with the additional use of an asymmetrical cipher;

Fig. 4 shows a configuration with Vernam cipher;

Fig. 5 shows a further version with Vernam cipher;

Fig. 6 shows a configuration with external crypto-module; and

Fig. 7 shows a further configuration with crypto-module.

The reference characters/abbreviations used in the appended list are employed in the Drawing, in the following description, in the Patent Claims and in the Abstract.

DETAILED DESCRIPTION

Fig. 1 shows a Vernam cipher in simplified form. The

encryption process, identified here by "V", may be a very simple mathematical operation, such as EXOR, which also allows broad-band encryption in software, i.e., without the support of a special crypto-hardware. ~~The~~ disadvantage ~~of such known methods~~, however, is that the message, indicated by "TEXT", must be encrypted using a Vernam key KV ~~composed~~ of a random number having the length of the message to be encrypted. Consequently, long Vernam keys are required for long messages. This means that the Vernam cipher can only be used to a limited extent for practical applications. Fig. 2 shows a modern symmetrical cipher S, such as DES or IDEA, which also still provides excellent security in the case of relatively short key lengths, ~~usually~~ 128 bits for the secret symmetrical key KS. DES and IDEA, respectively, are data encryption standards (ANSI and ASCOM) ISO 9979. Here too, however, as in the case of the Vernam cipher, the secret key KS required for encryption and decryption must be exchanged via a secure channel, independent of the transmission path used for the message, for example with the aid of a courier. The configuration shown in Fig. 3, which is described in detail in the literature source indicated in the introduction, has avoided this disadvantage through the additional use of an asymmetrical cipher A, for example the RSA method, for the transmission of the secret encryption key KS. In this case, the encryption key KS is encrypted with the public asymmetrical key KAp of the recipient and can subsequently be decrypted again by the recipient using his secret symmetrical key. The public recipient key KAp ~~required~~ for this purpose at the sender's end can be transmitted to him by the recipient over any insecure channel. Of course, the message could also be encrypted directly with the public recipient key KAp, but the

achievable performance of the hardware and software available for an asymmetrical cipher is significantly lower than in the case of a symmetrical cipher, so that in the case of long messages and to attain a high processing speed, use is made of the asymmetrical and symmetrical ciphers, usually in the combination shown in Fig. 3, namely a hybrid method. In Fig. 4, the encryption of a secret parameter IV of variable length, for example, n · 180 bits, with a symmetrical key KS, for example, 128 bits, results in the generation of a very long (pseudo)-random number which, as Vernam key KV, finally encrypts the message to be protected. For transmission of the encryption/ decryption key to the recipient, however, the courier in this case does not need to transport the Vernam key KV, but merely the key KS and the parameter IV, from which the Vernam key KV can easily be simulated on the recipient's side, because the same configuration exists here as on the sender's side. Fig. 5 shows encryption using combined asymmetrical, symmetrical and Vernam ciphers, as in Fig. 4. In contrast to Fig. 4, which requires a courier for exchanging the secret key information, according to Fig. 5 an asymmetrical cipher is used for this purpose, analogous to Fig. 3. The public recipient key KAp is fed in on the sender's side and the asymmetrical sender key KAs on the recipient's side.

The advantage of this procedure is made apparent in Fig. 6 and Fig. 7. The upper halves of Fig. 6 and Fig. 7, therefore, each show two ~~typical~~ terminal configurations. The gray-shaded elements represent the external crypto-hardware, including, for example, ~~composed~~ either of a chipcard or of a multifunctional PC interface adapter or PCMCIA module with built-in special crypto-hardware or a built-in

special chipcard. The encryptor, on the other hand, is implemented as a conventional PC, with software or another terminal which, however, with the exception of the very simple Vernam cipher, such as, for example, EXOR, that can be implemented even for broad-band applications in software, requires no further crypto-technology. Fig. 6 and Fig. 7 both show that the external crypto-modules are capable of taking on all the complex crypto-functions, generating the Vernam key KV, so to speak, as reserves and storing them in a suitable intermediate storage, the KV storage, until they are gradually used up by the encryption process through the logic operations V. The KV storage may be installed either in the personal computer or terminal, or also in the crypto-module in the form of a chipcard or PCMCIA module. The advantage of the devices according to Fig. 6 and Fig. 7 is that the encryptor is always able to operate with the same Vernam cipher, even if the external crypto- or PCMCIA modules use different symmetrical and asymmetrical ciphers. The Vernam cipher can also be implemented in software for high throughput rates, so that all encryptors are able to get along without expensive crypto-hardware and can be mass-produced at low cost. The external crypto-modules likewise remain competitively priced because the Vernam key, produced in reserve, can also be generated by a low-performance, i.e., low-speed chipcard, for example, for reserve in the KV storage, without slowing down the actual broad-band encryption process which operates independently thereof.

Because of the method described herein, the encryptors are freed from the problems of expensive, high-performance and mutually incompatible crypto-hardware. On the other hand, the Vernam cipher can be implemented very simply and inexpensively in software. All the

complex crypto-functions are located outside of the encryptor. The great advantage is also that they are interchangeable by module and can be implemented in the ~~proposed,~~ competitively priced and low-speed external crypto-modules, such as, for example, a chipcard or a PCMCIA card. The methods used are negotiated or signaled during coordination between sender and receiver, for example, on the transmission path.

The method for the low-cost implementation even of high-performance encryption functions in an encryptor which may be composed merely of PC software or any other terminal/information system with integrated Vernam cipher that does not need to be supported by expensive crypto-hardware for the actual encryption process has the distinction that, with the aid of a secret key KS having a defined key length and using a variable parameter having a defined bit length, a Vernam key KV having the length of the message to be encrypted is generated by way of any symmetrical cipher S, the Vernam key KV, on its part, encrypting the message to be protected by way of the Vernam cipher, the secret key KS and the parameter IV being communicated from the sender to the recipient either via a secure channel separate from the message-transmission path, or directly on the message-transmission path, for example, secured by an asymmetrical method A, the recipient regenerating the Vernam key KV using the above-described method in order to be able therewith to decrypt the received message. The symmetrical and, optionally, also the asymmetrical cipher and, optionally, also the storage for the Vernam key, namely the KV storage, are accommodated in an external crypto-module separate from the encryptor, for example, in the form of a chipcard or PCMCIA module or the like,

while only the Vernam cipher and, optionally, the storage KV for the Vernam key remain in the encryptor.

List of reference characters

KV	Vernam key
V	Logic operation, such as EXOR
KS	Secret symmetrical key
S	Symmetrical cipher, such as IDEA
KAp	Recipient key (asymmetrical)
KAs	Sender key (asymmetrical)
A	Asymmetrical cipher
IV	Secret variable parameter
PCMCIA	Multifunctional PC interface adapter
PC-SW	PC software